SUBMISSION

Submission to APRA — Strengthening operational risk management

21 October 2022

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2022/18

General Manager, Policy

APRA

Via email: PolicyDevelopment@apra.gov.au

21 October 2022

Dear Sir/Madam

Strengthening operational risk management

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to APRA's discussion paper *Strengthening operational risk management* and the draft CPS 230 *Operational Risk Management*.

About ASFA

ASFA is a non-profit, non-partisan national organisation whose mission is to continuously improve the superannuation system, so all Australians can enjoy a comfortable and dignified retirement. We focus on the issues that affect the entire Australian superannuation system and its $3.3 trillion in retirement savings. Our membership is across all parts of the industry, including corporate, public sector, industry and retail superannuation funds, and associated service providers, representing almost 90 per cent of the 17 million Australians with superannuation.

*****

If you have any queries or comments in relation to the content of our submission, please contact Julia Stannard, Senior Policy Advisor, on (02) 8079 0838 or by email jstannard@superannuation.asn.au.

Yours sincerely

Julian Cabarrus

Director – Policy Operations, Member Engagement & External Relations

Table of contents

A. General comments and executive summary

ASFA welcomes the release of draft CPS 230 *Operational Risk Management*. The proposed standard is an important addition to the prudential framework and reflects the need to ensure APRA-regulated entities apply an appropriate level of maturity and sophistication when dealing with operational risks.

The changes to risk management practices outlined in the draft standard are substantial and their implementation will involve considerable effort on the part of regulated entities and their service providers.

ASFA's submission and recommendations focus on the impacts of CPS 230 on the APRA-regulated superannuation sector, and address five key themes.

Recommendations

1. To allow adequate time for implementation and avoid creating an excessive compliance cost and burden:
    - CPS 230 should not commence until at least 12 months after the publication of the finalised standard and the associated guidance, with compliance required for material service provider arrangements entered into, or materially amended, from that date
    - regulated entities should then have until a specified date – at least three years after the publication of the finalised standard and the associated guidance – to review existing arrangements, bring them into alignment with the standard, and notify APRA where any arrangements will not be compliant by the specified date.
2. The scope of the 'material service provider' concept should be refined to ensure only arrangements that are genuinely material to the regulated entity are captured. We suggest an appropriate definition would be:

    Material service providers are those on which the entity relies to undertake a critical operation **and** that expose it to material operational risk.
3. CPS 230 should be refined to more clearly reflect that while a regulated entity's Board is ultimately accountable for the *oversight* of operational risk management, its management is responsible for the *ownership and management* of operational risk across the entity's end-to-end processes.
4. To avoid confusion, APRA should provide clarity about the relationship between APRA's suite of prudential requirements and guidance that deal with risk.
5. To ensure all regulated entities share a common understanding of its expectations in relation to the CPS 230 requirements, APRA should address in the final version of the standard and the accompanying guidance the points of clarification requested in this submission.

A.1. Ensuring the commencement date and transition arrangements are reasonable and appropriate

ASFA is concerned that 1 January 2024 may not be a reasonably achievable commencement date for CPS 230, given APRA does not expect to finalise the standard, and begin consultation on guidance material, until early 2023. The effort required from regulated entities in order to comply with the new standard will be extensive and time consuming. Some aspects of the necessary work cannot be completed – or, in some cases, commenced – until the final requirements and guidance have been settled.

In addition, ASFA considers it will be critical to provide appropriate transition arrangements to avoid creating a bottleneck situation where all APRA-regulated entities, and all their service providers, must attempt to simultaneously renegotiate large numbers of agreements to ensure compliance by the commencement date of the standard.

In ASFA's view, the commencement date for CPS 230 should be at least 12 months after the publication of the finalised standard and the associated guidance, with compliance required for material service provider (MSP) arrangements entered into, or materially amended, from that date. Regulated entities should then have until a specified date – at least three years after the publication of the finalised standard and the associated guidance – to review existing (pre-commencement) MSP arrangements and bring them into alignment with the standard and notify APRA about any arrangements that will not be compliant by the specified date. This would significantly reduce the potential implementation costs associated with the new standard, allowing regulated entities to bring most of their pre-existing arrangements into compliance as they come up for renewal.

For further comments on this matter, please refer to our response to consultation question 8 in section B below.

Recommendation 1

To allow adequate time for implementation and avoid creating an excessive compliance cost and burden:

- CPS 230 should not commence until at least 12 months after the publication of the finalised standard and the associated guidance, with compliance required for material service provider arrangements entered into, or materially amended, from that date
- regulated entities should then have until a specified date – at least three years after the publication of the finalised standard and the associated guidance – to review existing arrangements, bring them into alignment with the standard, and notify APRA where any arrangements will not be compliant by the specified date.

A.2. Ensuring key concepts are appropriately scoped: 'material service provider' and 'critical operation'

The concepts of 'material service provider' (MSP) and 'critical operation' are fundamental to CPS 230 – they underpin many of the requirements outlined in the draft standard. Given their significance, it is imperative that these concepts are clearly understood by regulated entities and that they are scoped appropriately.

We acknowledge that APRA intends to release a prudential practice guide to accompany CPS 230, and this will likely provide further clarity around these concepts. However, in ASFA's view the way both concepts are reflected within the draft standard itself can and should be improved.

ASFA considers there is a lack of clarity in the draft standard. Further, the inclusion of prescriptive but non-exhaustive lists of MSPs and critical operations undermines the high-level, principles-based definitions and fails to recognise that what is 'material' or 'critical' for one regulated industry - or even one regulated entity – may not be genuinely 'material' or 'critical' to the business continuity of another.

The adopted approach means the concepts of MSP or critical operation are capable of being interpreted extremely widely. This will increase the range and number of service provider arrangements that regulated entities treat as subject to the enhanced standards, potentially beyond what was actually intended by APRA. This will have a direct impact on the transition time required by entities and will also considerably increase the compliance burden and cost associated with the standard.

For further comments on this matter, please refer to our response below to consultation questions 5 and 6 in section B below.

Recommendation 2

The scope of the 'material service provider' concept should be refined to ensure only arrangements that are genuinely material to the regulated entity are captured. We suggest an appropriate definition would be:

> Material service providers are those on which the entity relies to undertake a critical operation **and** that expose it to material operational risk.

A.3. Clarifying Board and senior management accountability

ASFA appreciates that APRA is seeking to increase the role that the Boards of regulated entities play in relation to risk management. We acknowledge that an increased focus on an entity's operational resilience, *before* operational risks have crystallised, should increase the capability of the entity to withstand severe/extreme disruptions when risk appetites are likely to have been exceeded.

However, for some aspects of the draft standard we question whether the correct balance has been struck between Board and senior management accountability. In particular, we are concerned that the draft standard appears to extend the Board's role to approval of specific processes and in some instances responsibilities appear to cross over between the Board and management.

We note that the drafting of the standard does not appear to allow for delegation of Board functions to Board committees, as is common practice.

We further note that page 18 of the Discussion Paper indicates that the draft standard reflects a principles-based approach reflecting the respective roles of the Board and senior managers. This includes the statement that "senior managers within the business are responsible for the ownership and management of operational risk across an entity's end-to-end processes". This does not, in ASFA's view, appear to be the approach taken for some requirements in the draft standard, where functions are assigned to the Board that appear more appropriate for senior management – for example:

- approval of the individual tolerance levels for disruptions to each critical operation
- review of the risk and performance reporting on MSP arrangements
- decisions related to MSP arrangements, including changes to arrangements.

Requiring the Board to devote attention to specific operational processes at this level of detail has the potential to detract from their core role of providing strategy and direction.

ASFA considers these are matters more appropriate to be left with senior management, with the Board setting the overall risk tolerance, approving the risk management framework and providing oversight (directly or through its sub-committees) as appropriate. These matters should be appropriately reflected in a robust delegations framework that reflects operational reality.

Recommendation 3

CPS 230 should be refined to more clearly reflect that while a regulated entity's Board is ultimately accountable for the *oversight* of operational risk management, its management is responsible for the *ownership and management* of operational risk across the entity's end-to-end processes.

A.4. Avoiding uncertainty caused by overlap with other prudential requirements

Draft CPS 230 directly or indirectly raises several concepts that are addressed in other prudential standards - in particular, SPS 220/CPS 220 *Risk Management*, CPS 511 *Remuneration* and CPS 234 *Information Security*. This has the potential to cause confusion as to whether certain standards take precedence over others.

ASFA considers it would be helpful for APRA to provide clarity about the relationship between APRA's suite of prudential requirements and guidance that deal with risk. This would assist regulated entities in understanding how requirements across different standards intersect. We recommend that this be outlined in a standalone document, rather than incorporated into CPS 230, so it may be more readily updated as the prudential framework continues to evolve.

In addition, we understand that it is APRA's present intention to keep its requirements in relation to outsourcing to a cloud computing service provider separate from CPS 230. ASFA recommends that APRA reconsiders this approach, which is likely to cause confusion. In ASFA's view all requirements in relation to the outsourcing of a critical function should be integrated into CPS 230 or, at a minimum, there should be reference to any separate requirements for particular functions within CPS 230.

Recommendation 4

To avoid confusion, APRA should provide clarity about the relationship between APRA's suite of prudential requirements and guidance that deal with risk.

A.5. Ensuring the requirements of CPS 230 are clear, to promote consistency of application

It is important that all regulated entities share a common understanding of APRA's expectations in relation to the requirements outlined in CPS 230.

Our response to consultation question 2 in section B below raises some matters which are not addressed in the draft standard. We have also included, in section C, an extensive list of specific aspects of draft CPS 230 where we consider further clarification is necessary within the standard and/or the accompanying guidance or would help to ensure the consistent application of the requirements across all APRA-regulated industries.

Recommendation 5

To ensure all regulated entities share a common understanding of its expectations in relation to the CPS 230 requirements, APRA should address in the final version of the standard and the accompanying guidance the points of clarification requested in this submission.

B. Comments in response to APRA's consultation questions

Q1. Is a single cross-industry standard for operational risk management supported?

ASFA members are generally supportive of a single standard applying to APRA-regulated entities.

However, we note that there are some nuances between the different regulated industries that may make the interpretation and application of a genericised standard challenging for regulated entities. For example:

- entities within the APRA-regulated superannuation industry are likely to have a substantially higher number of MSP arrangements than entities in other regulated industries
- the service provider categories and operations included in the prescriptive lists of MSPs and critical operations will not be equally relevant to the various regulated industries.

These industry nuances mean it will likely be necessary for APRA to:

- introduce into the standard some layers of requirements to reflect the genuine differences between the different regulated industries
- provide, within its guidance material, additional commentary and/or examples addressing how the requirements apply to a particular industry.

Otherwise, it is likely that regulated entities may expend unnecessary time and effort seeking to apply the requirements to their operations to an extent not intended by APRA.

Q2. Are there specific topics or areas on which guidance would be particularly useful to assist implementation?

As noted in section A.4. of this submission, ASFA is concerned that the overlap between draft CPS 230 and other prudential standards creates unnecessary confusion for regulated entities. We recommend that APRA clearly outlines the relationship between APRA's suite of prudential requirements and guidance that deal with risk.

ASFA's members have provided extensive feedback highlighting areas that we consider warrant clarification in the final version of CPS 230 itself, or coverage in the guidance material that APRA will provide to accompany the standard. These are detailed, with reference to specific aspects of the draft CPS 230, in section C of our submission.

We are strongly of the view that definitions or fundamental clarifications of significant concepts should appear in the standard itself, rather than the guidance, given the guidance is intended to inform an entity regarding the requirements in the standard to which it will be held.

ASFA notes the use of related party service providers and the increasing trend within the superannuation industry toward insourcing of some key services that may previously have been fully outsourced, for example investment management or fund administration. These matters are not addressed within the draft standard. ASFA members would appreciate clarity as to how:

- APRA's expectations in relation to oversight of 'insourced' service provision align with the requirements outlined in CPS 230
- CPS 230 should be viewed in relation to service provision by related parties, including in circumstances where a registrable superannuation entity (RSE) and responsible entity have common agreements.

We also note that many service providers to the superannuation industry are not themselves APRA-regulated – including some custodians.

Where those service providers specialise in providing services to the superannuation industry (or other regulated industries), it is expected they will have awareness of CPS 230 and will be prepared to make reasonable efforts to assist regulated entities in bringing the service provider agreement into alignment with the standard. However, ASFA envisages that regulated entities may face challenges when seeking to renegotiate arrangements with some other service providers, for example custodians or investment, venture capital, private equity or hedge fund managers in jurisdictions outside Australia where the regulatory requirements differ to APRA's. These are important providers of services to RSEs and any outcome where RSEs were not permitted to engage them would be problematic.

Some providers not regulated by APRA may be subject to ASIC regulation (for example, some providers of custodial services). ASFA strongly encourages APRA to liaise with ASIC to identify any regulatory levers that may be utilised to assist in the transition to CPS 230 compliance. This might include, for example, exploring whether there is scope to expand Regulatory Guide RG 133 *Funds management and custodial services: holding assets* to require ASIC regulated custodians to meet APRA's requirements under CPS 230 where they are providing services to APRA-regulated industries. At a minimum, there will need to be close liaison between APRA and ASIC to ensure their expectations are aligned.

Finally, ASFA members have noted they would find significant value in APRA making available de-identified data about the range of operational risk events and impacts it has observed or been notified of. ASFA considers this would provide considerable assistance to regulated entities in ensuring they are correctly interpreting and applying the requirements of CPS 230 in the implementation phase. Going forward, the increased notifications under CPS 230 mean APRA will have access to very detailed operational risk information across its regulated industries. This information could provide considerable assistance to regulated entities in terms of managing their risks on an ongoing basis. We recommend that APRA outlines how it will engage with industry to share learnings in this area.

Q3. How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?

ASFA considers that greater clarity is needed around the key concepts of 'material' services providers and 'critical' operations (see section A.2 and our responses to consultation questions 5 and 6). This will enable regulated entities to better understand the extent to which particular requirements in the draft standard may apply to their operations.

Beyond that, we note that the 'objectives and key requirements of this Prudential Standard' section on the cover page of the draft standard notes that:

> "An APRA-regulated entity's approach to operational risk must be appropriate to its size, business mix and complexity."

While this suggests a level of proportionality, the tone is not carried through to the body of the standard – the drafting of the various paragraphs adopts prescriptive language that would appear to apply the requirements to all regulated entities, regardless of their size, business mix or complexity.

ASFA recommends that APRA includes, in the body of the standard, a clear statement to the effect that a regulated entity's size, business mix and complexity can be taken into account when applying the requirements of CPS 230. ASFA further recommends that APRA makes it clear this means some requirements may not apply to a regulated entity.

Once that clarity has been provided, ASFA considers the requirements should apply to all APRA-regulated entities, regardless of whether they are significant financial institutions (SFIs) or not. We note that smaller and/or less complex entities are not immune from operational risk and may be less resilient in absorbing its impact.

ASFA also considers that the guidance material should include practical examples and guidance (including examples drawn from real life) for RSEs with differing business/operating models, outlining what APRA considers to be critical operations, tolerance levels and material service providers.

Q4. What are the estimated compliance costs and impacts to meet the new and enhanced requirements?

Given the level of uncertainty as to the scope of the final requirements, ASFA members have found it extremely difficult to estimate the potential cost of compliance with CPS 230. However, it will clearly involve substantial monetary and resource cost both in the implementation phase and ongoing.

In preparing to comply with the requirements of CPS 230, some of the activities an APRA-regulated superannuation entity will need to undertake include:

- an extensive once-off process to identify existing MSPs and fourth parties, then review and renegotiate existing MSP arrangements to bring them into alignment with CPS 230 – this:
    - is likely to involve significant time/cost for internal and external legal resources
    - will also require substantial input from business units regarding services provided to the entity and their criticality, including risk owners within the business units and procurement/sourcing teams
    - may involve an increase in the amount payable under MSP arrangements as service providers seek to 'price in' additional work to align with CPS 230
- upgrading systems, including to integrate information across multiple information systems and ensure data quality
    - uplifting policies/governance documents, standard contracts/agreements with service providers, service provider selection and on-boarding processes, service provider relationship and performance management, monitoring controls to track implementation and ongoing compliance, processes to deliver timely and relevant reporting/information on operational risk to the Board
    - a training and capability uplift for personnel, particularly risk owners/managers, Board and senior management.

One ASFA member (an APRA-regulated superannuation fund) has indicated the implementation of CPS 230 will require significant cost in terms of execution effort, primarily impacting legal, procurement, management and enterprise risk and compliance specialists supported by project management, business analysis and training and development.

Another ASFA member (an APRA-regulated superannuation fund) has indicated the standard will apply to far more procurement projects than the current prudential requirements and will add significant complexity and time to the procurement and supply management process, especially in relation to technology procurement. The member estimates that it will require additional resourcing for a period of up to 24 months to implement the requirements of the standard across its procurement functions, with an increased ongoing workload yet to be estimated.

On an ongoing basis (that is, post-implementation), ASFA members see an increased workload for internal and external legal resources, procurement/sourcing teams and finance/internal audit, given the potential increase in MSP arrangements that will require internal audit review. It will not be possible to definitively establish the number of MSP arrangements an RSE will have until CPS 230 and the associated guidance has been finalised. However, preliminary estimates provided by ASFA members include one large superannuation provider moving from 17 material outsourcing arrangements under the current requirements to **over 100** MSP arrangements under CPS 230, and another moving from 5 material outsourcing arrangements currently to **over 60** MSP arrangements under CPS 230.

To the extent CPS 230 adds to the overall compliance burden on funds there will also likely be opportunity cost, in the sense that fewer resources will be available to devote to other strategic priorities, including initiatives to add value to fund members.

Parties external to the fund may also face compliance costs and impacts – for example, MSPs and fourth parties may incur increased cost/effort to enable an APRA-regulated fund to meet the enhanced requirements under CPS 230.

Q5. How could APRA improve the definitions of critical operations, tolerance levels and material service providers?

Q6. What additions or amendments should be made to the lists of specified critical operations and material service providers?

ASFA considers there is need for a greater level of clarity - within the standard, not simply the guidance material – about the concepts of MSP and critical operation. If regulated entities do not have confidence in what is intended to be caught by these definitions, this will likely lead to entities applying the enhanced requirements to a broader range of service providers than is actually intended by APRA. This will significantly add to the compliance cost and burden associated with the standard.

The draft standard provides a high-level definition of 'material service provider' (MSP) and 'critical operation' (paragraphs 34 and 48 respectively), using a principles-based approach. ASFA considers this approach is effectively undermined by paragraphs 35, 49 and 50, which provide non-exhaustive lists of operations and services providers that APRA deems to be 'critical' and 'material'. ASFA members are of the view this:

- creates confusion between the concepts of MSP and critical operation
- fails to account for differences between the entities to which draft CPS230 would apply.
- appears to be at odds with the comment in the Discussion Paper (page 21) that "it is the responsibility of the entity to define, identify and maintain a register of its critical operations".

The definition of MSPs currently proposed in the draft CPS 230 is as follows (our emphasis):

> Material service providers are those on which the entity relies to undertake a critical operation **or** that expose it to material operational risk.

We consider that this definition is excessively broad and, to an extent, conflates the concepts of MSP and critical operation. The provision of what APRA has deemed to be a 'critical operation' will not, in ASFA's view, always be genuinely 'material' to a regulated entity and therefore the provider should not automatically be deemed to be an MSP. An entity may have many service providers providing a particular critical operation. In these circumstances, the failure of one individual service provider may not present a risk to business continuity.

For example, we accept that investment management is, for an APRA-regulated superannuation fund, a 'critical operation' as specified in paragraph 35. However:

- a fund will typically engage a significant number of investment managers, some of which may manage an amount that cannot, when considered against the total funds under management, be considered 'material'
- deeming all investment management arrangements to be automatically 'critical' – and therefore subject to the requirements of CPS 230 – will potentially mean an RSE is unable to directly undertake some investments that it would currently undertake utilising a risk-based approach. ASFA members have indicated they anticipate that venture capital, start ups and some overseas operations that fall

under different regulatory requirements (such as the EU's Alternative Investment Fund Managers Directive) will resist compliance with APRA's requirements.

We consider that an RSE licensee should be able to assess materiality in a risk-based manner, reflecting the genuine potential impact to fund members and allowing for a cost/benefit approach to be applied.

We recommend that the definition of MSP be redrafted as follows:

> Material service providers are those on which the entity relies to undertake a critical operation **and** that expose it to material operational risk.

It is also important to recognise that particular operations, or particular categories of service, may have different levels of importance depending on the industry in which a regulated entity operates. As a result, what is 'critical' or 'material' for entities in one regulated industry may not be genuinely critical or material for entities in another. In ASFA's view, this makes the adoption of a prescriptive list of critical operations and MSPs problematic. We recommend that paragraphs 35 (critical operations) and 49 (MSPs) be redrafted as examples of operations and service provider categories that may be critical/material for a regulated entity, rather than prescriptive lists.

In terms of additional guidance, the Discussion Paper indicates APRA has had regard to international standards and international peers' approaches and guidance in developing the draft CPS 230. In this respect, ASFA considers the United Kingdom's recently finalised requirements in relation to building operational resilience to be particularly relevant. It would be helpful for Australian regulated entities to understand the extent to which APRA may be guided by learnings from the UK, in particular the findings from the initial assessment by the Prudential Regulation Authority (PRA) of UK entities around their identification of 'important business services' (effectively, the equivalent to the 'critical operations' concept in draft CPS 230). We note the PRA found that the level of granularity at which financial firms had identified their important business services had varied widely, and as a result it provided further clarification of its expectations. In ASFA's view, this demonstrates the need to ensure the CPS 230 requirements are drafted in a way that ensures APRA's expectations are clearly understood, from the outset, by all regulated entities.

Q7. Are the notification requirements and the time periods reasonable?

ASFA notes that draft CPS 230 outlines four requirements for regulated entities to notify APRA about an event, each with a different notification timeframe:

1. Paragraph 32 requires notification within 72 hours after becoming aware of an operational risk incident that is likely to have a material financial impact or a material impact on the entity's ability to maintain its critical operations
2. Paragraph 41 requires notification within 24 hours if an entity has activated its BCP
3. Paragraph 58(a) requires notification within 20 business days after entering into or materially changing an agreement for the provision of a service relied upon to undertake a critical operation
4. Paragraph 58(b) requires notification prior to entering into any offshoring agreement with an MSP or when a significant change is proposed to such an agreement.

These are in addition to existing reporting obligations for APRA-regulated funds, including requirements under which an RSE licensee must:

- notify APRA within 10 business days when it becomes aware of a significant breach or a material deviation from the risk management framework (RMF), or discovers that the RMF did not adequately address a material risk: SPS 220 paragraph 35

- report to APRA within 30 days after becoming aware of a breach of a RSE license condition, including a breach of the RSE licensee law (which includes prudential standards): sections 29E/29JA/10(1) of the *Superannuation Industry (Supervision) Act 1993*
- report to ASIC within 30 days after becoming aware of a reportable situation: section 912D of the *Corporations Act 2001*, RG 78 *Breach reporting by AFS licensees and credit licensees*.

The multiplicity of overlapping notification/breach reporting requirements is likely to cause confusion and will add to the compliance cost for regulated entities. Further, given some of the notifiable events under draft SPS 230 may already be reportable/notifiable under an existing regulatory requirement, there will also be a regulatory impact for APRA and/or ASIC.

ASFA is of the view consideration should be given to aligning and streamlining notification/reporting requirements wherever possible. In addition, APRA should provide clear guidance to regulated entities on how they are intended to comply with overlapping notification/reporting requirements, framed with a view to minimising duplication of effort for both regulated entities and regulators alike.

With specific reference to paragraph 32 – the requirement to notify APRA within 72 hours after becoming aware of an operational risk incident that is likely to have a material financial impact or a material impact on the entity's ability to maintain its critical operations – ASFA notes that this is a relatively short timeframe. We anticipate that the level of information able to be reported within 72 hours, while the entity is focussed on remediating/recovering from the incident, may be quite preliminary in nature. We acknowledge that it is consistent with the timeframe applicable under CPS 234 for reporting of information security incidents. We recommend that before adopting the requirement in CPS 230, APRA should review whether, in practice, the data provided within 72 hours under CPS 234 is a meaningful contribution to APRA's supervisory activities or whether more value would be gained from a slightly longer reporting timeframe.

Q8. What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers [if required]?

APRA has indicated 1 January 2024 as the commencement date for the new standard – some 14 months away. However, as APRA does not expect to finalise the standard until "early 2023" and it is not clear when finalised guidance may be released, the effective timeframe to commencement is likely to be very much shorter.

Given the potential for changes to the requirements as a result of this consultation process, and the need to await guidance to expound on concepts raised in the standard, it may not be practicable for regulated entities to begin the process of renegotiating service provider arrangements until at least mid-2023, possibly later.

ASFA takes the view that a commencement date of 1 January 2024 is likely to be impracticable. ASFA considers that a timeframe to commencement of at least 12 months should be provided from the date that all final requirements and guidance have been published.

In addition, regardless of the ultimate commencement date for the standard, transition arrangements will be necessary and must be reasonable, reflecting the time needed to renegotiate service provider agreements. APRA-regulated superannuation funds are likely to have many agreements that will require renegotiation in order to comply with the standard.

We understand from discussions with APRA representatives that the current intention is to require all impacted service provider arrangements to be renegotiated to comply by the commencement date of SPS 230. ASFA considers this to be impracticable and overly burdensome on regulated entities and their service providers.

Requiring all impacted agreements to be renegotiated within a constrained timeframe will have a substantial compliance impact for regulated entities, adding considerably to the resource and monetary cost associated with the new standard. It will also cause a flow-on effect impacting entities' service providers, particularly given the extent of market concentration for many providers of services to APRA-regulated superannuation funds.

Further, regulated entities are likely to encounter significant issues in securing timely renegotiation of agreements where service providers are not APRA-regulated -including providers based overseas.

One ASFA member (a large APRA-regulated superannuation fund) has indicated that, given the volume of arrangements potentially impacted by CPS 230, it could take between one and three years to renegotiate and vary all existing service provider agreements to fully comply with the standard. This would require additional procurement resourcing as well as substantial legal resources and costs.

We recommend that a risk-based and phased approach is adopted.

We note that guidance as to appropriate transition timeframes can be drawn from implementation of similar requirements both in Australia and overseas.

Internationally, several jurisdictions that have adopted operational resilience reforms, or reforms more specifically addressing outsourcing, have taken a phased approach. For example, development and implementation of the United Kingdom's operational resilience standards took place over a period of several years. Regulated entities were required to identify their important business services (critical operations), set impact tolerances and carry out mapping and testing by March 2022, and must achieve full compliance by March 2025. In Ireland, a new outsourcing standard regulated by the Central Bank of Ireland was based on the European Banking Authority's *Guidelines on Outsourcing*. These applied from 30 September 2019 for all new or amended outsourcing arrangements. Regulated entities given until 31 December 2021 (or first renewal, if earlier) to review and amend existing arrangements and were required to inform the regulator if the review process was not finalised by that date.

When APRA initially introduced SPS 231 *Outsourcing*, it provided a set of well-considered and risk-based transition arrangements. Provided there was compliance from commencement with specified requirements, RSEs were essentially able to bring arrangements for existing outsourcings into full compliance as arrangements were renewed at expiry or replaced with new service providers.

We strongly recommend that a similar approach is adopted for CPS 230. In particular, we recommend that:

- the commencement date for CPS 230 should be at least 12 months after the publication of the finalised standard and the associated guidance, and compliance should be required for MSP arrangements entered into, or materially amended, from that date
- regulated entities should have until a specified date - at least 3 years after the publication of the finalised standard and the associated guidance - to:
    - review existing (that is, pre-commencement) MSP arrangements and bring them into alignment with the standard
    - notify APRA of any existing MSP arrangements that will not comply with the standard by the specified date, and the anticipated end-date of those arrangements.

C. Comments on specific aspects of CPS 230

Based on feedback from members, ASFA has identified numerous instances where:

- additional guidance, in the standard or accompanying guidance, would assist regulated entities; or
- we recommend that the current wording in draft CPS 230 is modified.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
11(a)	Requirement to effectively manage operational risk and set and maintain appropriate standards for conduct and compliance	The statement in para (a) is very general and arguably broader than the scope of the standard. Clarification is requested as to APRA's expectations, particularly in relation to 'conduct'.
12	Requirement to identify, assess and manage operational risks from inadequate or failed internal processes or systems, actions or inactions of people or external drivers and events.	• Without any reference to materiality, this statement is extremely broad, and it is unclear whether it is intended to duplicate existing requirements under SPS 220 (para 6 and 22(b)) or extend them. • The ability to identify a person's 'inaction' may be subjective without a loss event. Further clarification would assist interpretation of this requirement.
13	Regulated entity must, to the extent practicable, prevent disruption to critical operations	SPS/CPS 232 currently accept that disruptions occur and focus on an entity having the processes to manage through. While we note the inclusion of "to the extent practicable", the requirement in para 13 to "prevent" disruption appears to be a significant increase in the requirement. Clarification is requested of how this changes APRA's expectations, in particular in relation to an entity's service providers as any ability to "prevent" disruption is limited to embedding contractual arrangements and conducting due diligence and ongoing monitoring.
14	Regulated entity not to rely on a service provider unless it can ensure it can continue to meet prudential obligations in full and effectively manage associated risks	This statement is extremely broad. Confirmation is sought that this is limited to a regulated entity's core business/critical operations.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
15	Risk management framework	This para overlaps heavily with SPS/CPS 220 and is also much more generally expressed than the relevant paragraphs in standards it will replace (for example, SPS/CPS 232 regarding business continuity management). Clarification is requested of: • what additional expectations APRA has over and above the existing SPS/CPS 220 requirements • whether a risk profile is only required for operational risk • whether a regulated entity that is part of a group can adopt the group BCP where it addresses the requirements of the entity (as in SPS 232 para 5).
16	Review of entity's operational risk management	Para 16 specifically refers to SPS/CPS 220 in relation to the requirement to undertake a review of the RMF and states that the review "must cover the aspects of operational risk management set out in paragraph 15". This is despite operational risk already clearly being included as one of the categories of risk in SPS/CPS 220 that must be covered by an entity's RMF. Clarification is requested that para 16 is intended to stipulate, for operational risk, requirements that are *additional* to those in SPS/CPS 220.
17	Integration of operational risk management into the overall risk management framework and processes	Further clarification would assist regulated entities to address the perceived area of concern.
18	Risk management framework	Clarification is requested as to what is considered a 'material weakness'.
19 23	Roles, responsibilities and accountabilities	• See section A.3 of this submission for comments in relation to the role of the Board vs senior management. • Pursuant to para 19, the Board is *accountable* for the oversight of an "entity's operational risk management". Pursuant to para 23, senior management are "*responsible* for operational risk management". ○ Clarity is sought as to who is accountable for the *risk* ○ Clarification is sought as to the extent of the Board's obligation to oversee management of service provider arrangements – how far does this extend? Is it sufficient to address this in respect of the procurement policy and MSPs that may impact the core operations of the entity? ○ Is Board approval required or can this be delegated? ○ More guidance is sought in relation to senior management responsibilities ○ A consistent definition of 'senior management' should be applied across all entities

CPS 230 para	Issue addressed	ASFA comments/guidance sought
20	Board to set clear roles & responsibilities for senior managers	• Consideration should be given to whether inclusion of requirements in this standard in relation to accountability frameworks is appropriate, given these will be addressed by the Financial Accountability Regime. • Para 20 refers to 'senior managers' and footnote 8 indicates this term has the meaning given in SPS 520 in relation to RSE licensees, and in the Life Insurance Act in relation to life insurers: ○ this suggests the definition will not be consistent across all regulated industries ○ clarification is required of how this definition sits with the definition in CPS 511.
21	Board approval and oversight	• Approval of the BCP (para 21(b)) is more appropriately the role of senior managers rather than the Board. • Similarly, the obligation on Boards to review risk and performance reporting on MSP arrangements (para 21(c)) may be impractical. Decisions related to MSP arrangements, such as appointing, changing or ending an arrangement, should be left to senior management, with reporting and oversight provided by the Board and/or their sub committees as appropriate. • Further clarity/guidance is requested in relation to 'tolerance levels'.
22	Senior management to provide clear and comprehensive information to the Board on the expected impacts on the entity's critical operations when the Board is making decisions that could affect the resilience of critical operations.	• See section A.3 above for comments in relation to the role of the Board vs senior management. • Clarification is requested regarding the extent to which APRA expects the Board to be involved in the management decision versus the governance decision processes of an organisation. This requirement appears to blur the line between the roles of the Board and management. • Clarification is also required as to who is to provide this assessment in an outsourced model – confirmation is sought that the current responsible persons or delegates are able to provide this information.

CPS 230 para	Issue addressed	ASFA comments/guidance sought

23	Management of operational risks	• There is inconsistency between the 'operational risk' definitions applied in the proposed CPS 230 and SPS 114 *Operational Risk Financial Requirement Standard*, in particular in relation to reputational risk (our emphasis):
		  ○ para 23 of draft CPS 230 and page 12 of the Discussion Paper define operational risks as "risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events. Operational risk is inherent in all products, activities, processes and systems. It **includes** legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, **reputational risk** and change management risk"
		  ○ however, in SPS 114 (paragraph 6) operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk but **excludes** strategic and **reputational risk**".
		• The list of risk categories also does not align with SPS/SPG 220 – will APRA be amending SPS/SPG 220 to bring them into alignment?
		• Some of the descriptions are general terms that may overlap in assessing risk outcomes or represent a consequence of a risk event – for example:
		  ○ reputational damage is seen as a consequence rather than the root cause
		  ○ legal risk, regulatory risk, compliance risk may all also overlap and currently be captured by regulated entities under one category – what is APRA's expectation?
		• Senior management are responsible for operational risk management across the end-to-end process for all business operations. What is the expected depth and quality for understanding 'end-to-end' and does APRA expect this to be the same for all business operations?

24	Requirement to maintain appropriate and sound information and information technology infrastructure	Clarification is requested as to: • the relationship between this requirement and CPS 234 (is this duplicative or intended to impose an additional requirement?) • APRA's expectations in relation to 'sound' information and information technology infrastructure. • does the requirement apply only to systems owned by the regulated entity, or does it also apply to service providers?
25	Requirement to assess impact of business and strategic decisions on operational risk profile and operational resilience	Clarification is requested of APRA's expectations for this requirement – does it extend beyond what is currently addressed in a business impact statement, and should it correlate to the business Risk Appetite Statement?

CPS 230 para	Issue addressed	ASFA comments/guidance sought

26	Operational risk profile and assessment	• This requirement would appear to be covered by SPS/CPS 220; it is not clear why it is duplicated here.
		• Para (a) – it is unclear what APRA would consider to be 'appropriate and effective', clarification is requested.
		• Para (b):
		  ○ the extent of process mapping required is unclear, further clarification is requested (the more granular the requirement, the greater the compliance effort/cost involved)
		  ○ clarification is requested as to the level of detail expected where processes are outsourced to a service provider (related party or third party).
		• Para (c):
		  ○ clarification is required in relation to what 'scenario analysis' entails
		  ○ it is unclear whether this is intended to have a scope broader than the Operational Risk Financial Requirement scenario assessment and the BCP scenario testing and assessment processes.

27	Requirement to conduct a comprehensive risk assessment before providing a material service to another party	Clarification is requested as to whether APRA's concern here is limited to the provision of a material service by the regulated entity to another party, or whether it also extends to a regulated entity entering into an agreement with an MSP for the provision of a service to the regulated entity?
28	Design, implementation and embedding of internal controls	Clarification is requested as to: • APRA's expectations and whether explicit statements and metrics are required to comply with this requirement • whether the requirement is limited to the regulated party's controls or extends to controls of service providers.
29	Rectification of deficiencies in the control environment	Pursuant to paragraph 29, any gaps or deficiencies in the control environment must be rectified in a "timely manner". Adoption of a requirement to rectify within a "reasonable time" would recognise that the nature of any deficiencies may vary, and some may reasonably take longer to rectify than others.
30	Operational risk controls	Clarification is requested as to what is considered a 'material weakness'.
31	Requirement to take incidents and near misses into account in assessment of the entity's operational risk profile and control effectiveness 'in a timely manner'	Further guidance is required on what is considered an 'operational risk incident' (examples would be appreciated) and APRA's expectations in relation a 'timely manner'.

CPS 230 para	Issue addressed	ASFA comments/guidance sought

32	Notification to APRA of an operational risk incident	• Guidance is sought on:
		  ○ what would be considered a 'material operational risk' incident triggering the requirement to notify APRA within 72 hours
		  ○ whether the 72-hour timeframe commences from the point of identification or assessment of an operational risk incident
		  ○ how this notification requirement will operate alongside existing reporting obligations to APRA and ASIC
		  ○ whether the requirement applies only in relation to MSPs and BCP incidents
		  ○ the meaning of 'likely' impact.
		• While we acknowledge that CPS 234 also contains a 72-hour notification requirement, this is a relatively short timeframe. Before it is adopted in CPS 230, we recommend APRA reviews how the requirement is operating in practice under CPS 234.

33	Business continuity	• Para 33(c) requires maintenance of a 'credible' BCP – 'credible' is an extremely subjective term and requires clarification. • Does para 33(d) imply that BCPs must include an agreed BCP activation trigger in the event of a disruption? • Is para 33(e) intended to mean that *critical* operations must return to normal service levels promptly (noting that full operations may not return to normal for some time)?
34	Critical operations	See section A.2 and our response to consultation questions 5 and 6 above for comments in relation to 'critical operations'. Further guidance is sought on: • the scope of critical operations - the concept as expressed is high level and strategic, but at the granular level there will be many different material and non-material aspects of these critical operations. Does the BCP need to address only the material aspects of the critical operations? • whether the reference to the entity's "its role in the financial system" is intended only to apply to SFIs.
35	Prescriptive list of 'critical operations'	• See section A.2 and our response to consultation questions 5 and 6 above for comments in relation to 'critical operations'. • Further guidance is sought on APRA's expectations in relation to 'systems and infrastructure' and issues outside the control or influence of the regulated entity.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
37	Board approved tolerance levels for critical operations	• Additional guidance is requested in relation to quantifying the "maximum extent of the data loss the entity would accept as a result of a disruption" (para 37(b)). Is this intended to be aligned to another reporting standard/requirement, or is it for the regulated entity to define? • Para 37 appears to suggest tolerance levels must be established for each critical business function in isolation, however there may be flow on impacts to other critical functions if a single tolerance has been breached. It is unclear how this should be considered. • Confirmation is sought that tolerances for disruption of MSPs and critical operations are discretionary based on the scale and complexity of the operation. • Approval of the tolerance levels for disruptions to each individual critical operation is more appropriately the role of senior management, rather than the Board. The Board role should be limited to providing guidance as to tolerance levels generally. • Can critical function tolerance levels be treated as part of the RAS monitoring process, or does APRA require this to be a separate process? • Further clarity is requested around tolerance levels, including whether maximum allowable outages and recovery point objectives are all required to be documented.
38	APRA may require a regulated entity to review and change its tolerance levels for a critical operation	• Clarification is requested as to what is considered a 'heightened risk' or 'material weakness'. • It is unclear how APRA will be in a position to assess an entity's tolerance levels – if the intention is that entities' BCPs must be submitted to APRA, that has not been specified.
39	Contents of an entity's BCP	• CPS232 currently requires that the Board approves a regulated entity's BCM policy, however this requirement does not appear in CPS 230. Clarification is sought whether this is an intended omission. • The APRA discussion paper states (on page 25) specifies that a regulated entity would be required to submit its BCP to APRA on an annual basis, however this is not mentioned in CPS230 itself: ○ confirmation is sought as to whether or not this will be a requirement ○ assuming it will be a requirement – given APRA recognises that the entity may have multiple BCPs at different levels of the organisation, will the entity be expected to submit *all* BCPs to APRA on an annual basis?
41	Notification to APRA where entity has activated its BCP	Clarification is sought as to: • whether this requirement also applies where the BCP of an MSP and/or fourth party has been activated? If so, the 24-hour notification timeframe would be extremely difficult to meet • how the 24-hour notification for BCP activation works alongside the 72-hour timeframe for notification of a 'material operational risk' incident (para 32).

CPS 230 para	Issue addressed	ASFA comments/guidance sought
42-43	Testing and review program for entity's BCP	Clarity is sought as to APRA's expectations in relation to the testing program: • does the requirement that the testing program must include a range of severe but plausible scenarios apply to the entity's multi-year testing program (that is, it does not require multiple scenarios to be tested in the same year -noting that resourcing and cost impacts will be substantially higher if entities are not able to spread their testing of the range of scenarios over a period of years) • what form does APRA expect the testing to take – that is, desktop test vs full activation of the BCP vs scenario simulations?
45	Internal audit review of BCP and assurance to Board	Para 45 requires the internal audit function to periodically provide assurance to the Board that the BCP sets out a 'credible' BCP – 'credible' is an extremely subjective term and requires clarification.
47	Contents of entity's service provider management policy	• Lack of clarity around the concept of a 'material business activity', and how it differs from a 'critical operation', is likely to mean the concepts are applied differently across the industry. • Re para 47(a), does the register only need to contain a list of names of the entity's MSPs? If not, what additional detail is required? • Para 47(d) introduces the concept of 'fourth parties' that MSPs "rely on". The footnote elaborates slightly that a fourth party is "a party that a service provider relies on in delivering services to an APRA-regulated entity". This is extremely broad, as it does not involve any element of criticality or materiality to the service provision. More clarity is needed regarding: ○ the intended breadth of the 'fourth party' concept as presently it could be interpreted to include, for example, utility providers that the MSP relies on ○ how a regulated entity can demonstrate that it is managing its risks associated with fourth parties.
48 49	Managing material risk associated with using MSPs	• The concept of 'materiality' to be applied is not clear, other than by the category of services listed by APRA in para 49. There is no recognition that a service provider involved in providing a critical operation may not always be a 'material' service provider, for example where an individual provider is one of many providing a critical operation and its failure would not present a risk to business continuity. See section A.2 and our response to consultation questions 5 and 6 above for further comments in relation to the concepts of MSP and critical operation. • Further guidance is sought on: ○ how regulated entities should determine materiality/MSPs ○ what APRA means by 'core technology' ○ management of fourth parties - how far down the supply chain a regulated entity is expected to query an MSP where it concerns a material service category, as stipulated by APRA.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
52	Obligations on regulated entity before entering into, reviewing or materially modifying an arrangement with an MSP	• Re para (a), guidance is sought on APRA's minimum expectations in relation to the required level of due diligence. For example, does this mean that for every investment manager selection the RSE licensee or custodian is required to demonstrate why one manager was selected as opposed to another? • Para (c)requires a regulated entity to take reasonable steps to assess whether a service provider is "systemically important in Australia". With the exception of a few highly concentrated service areas, it is unlikely that a regulated entity will be in a position to make this assessment and it is unclear what consequences are expected to flow from it. Para (b) already requires consideration of the aspects of systemic risk that are likely to be relevant for the regulated entity, and it would appear APRA would be better placed to make any assessment of systemic importance in Australia. We recommend para (c) be removed.
53	Minimum requirements for MSP arrangements	• Para 53 does not include insurance, or confidentiality, privacy and security of information as minimum requirements (these are covered in SPS 231 para 21/CPS 231 para 29). Clarification is sought as to whether this is a conscious omission. • Para 53(c) – the requirement to include provisions to "ensure the ability of the entity to meet its legal and compliance obligations" is extremely broad – for example, the scope of "legal and compliance obligations" does not appear to be limited to those imposed by CPS 230. Unless this is qualified it is likely to have a significant impact on regulated entities' ability to negotiate service provider arrangements. • Para 53(d) requires "notification by the service provider of its use of other material service providers, through sub-contracting or other arrangements". Is this intended to align with modern slavery principles re investigation of the supply chain? • Para 53(e) requires the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider – this is extremely open-ended in scope. The drafting can be read as requiring service providers to negotiate unlimited liability under sub-contracting arrangements, which is more stringent than the requirement that applies between the regulated entity and the MSP itself (which simply requires that the contract covers liability). Such a requirement could require that MSPs renegotiate contracts (and liability clauses) with sub-contractors before being able to commence negotiating with regulated entities. Unless it is qualified, this requirement is likely to have a significant impact on contract pricing and may mean that MSPs will choose not to engage constructively in relation to implementation of CPS 230. For highly concentrated service areas where some providers are not themselves regulated by APRA (for example, custody), this would present genuine challenges for regulated entities.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
		• Para (g) requires RSE licensees to include in an agreement with an MSP the right "to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries (refer to section 52(2)(c) of the SIS Act)". Para (g) should adopt the language used in section 52(2)(c) – that is, referring to the "exercise of powers and performance of duties" rather than "acting" in the best financial interests of members. It is also unclear what value this contributes in relation to termination specifically, given the duty applies broadly already.
56	APRA power to require entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns	Clarification is requested regarding the circumstances in which APRA envisages it might use this power. We note that the potential exercise of this power would introduce a significant level of uncertainty into the contract negotiation. It is unlikely any service provider would agree to give regulated entities a unilateral and unlimited right to amend the contract. We recommend this is limited to a requirement that the regulated entity take reasonable steps or make its best endeavours to make changes to the MSP arrangement.
57	Monitoring and reporting on MSP arrangements	See our response to consultation questions 5 and 6 in section B above for comments about MSPs – the broader the interpretation of the concept, the greater the resource effort and compliance cost that will be associated with this requirement.
58	Notification to APRA in relation to a new agreement for a service relied on to undertake a critical operation (or a significant change to an agreement) or an offshoring agreement with an MSP (or significant change to an offshoring agreement)	• Clarification is sought as to the threshold for a 'significant change' that would require notification to APRA pursuant to para 58(b). • See section A.2 and our response to consultation questions 5 and 6 above for comments about the concepts of MSPs and critical operation. Notification of a significant change to an agreement would undoubtedly be meaningful for key service providers, such as a fund's custodian or administrator. However, while draft CPS 230 deems some service arrangements to involve an MSP, not all providers of that service will genuinely be 'material' to a regulated entity and we question the value to be derived from notifying APRA about changes, even significant changes, to such agreements. • For example, under para 49 providers of 'investment management' are deemed to be MSPs however an APRA-regulated superannuation fund may have over one hundred investment managers and some may manage amounts that cannot, given the total funds under management, be considered 'material'. It is not clear what value would be derived from notification to APRA of a change to an agreement with such an investment manager. However, the requirement has the potential to add considerably to the compliance burden and cost experienced by the regulated entity. • Clarification is further requested that the notification requirement is limited to where the service provided is itself critical and not merely where a service provider *contributes* to the provision of a critical operation.

CPS 230 para	Issue addressed	ASFA comments/guidance sought
		• Clarification is requested as to how CPS 230 sits with existing requirements around consultation with APRA in relation to the use of cloud computing services.
59	Internal audit review and reporting in relation to outsourcing arrangements with an MSP for a critical operation	• If the expectation is that internal audit reviews all proposed outsourcing to an MSP this will have a material impact on the workload of the internal audit team. Clarification is required as to whether this requirement also to material changes to MSP arrangements. • Para 59 contains the first usage, within CPS 230, of the term 'outsourcing'. Given the shift in focus away from 'outsourcing' (SPS 231) to 'service provision' (CPS 230), clarification would be appreciated as to whether the use of the term 'outsourcing' in para 59 is intended to have any special context. • Clarification is requested as to APRA's expectations in relation to the internal audit function 'regularly' reporting to the Board/Board Audit Committee – is reporting as part of a 3-year audit cycle adequate?